


This is a copy of a chat between Claude and Sam. Content may include  unverified or unsafe content that do not represent the views of Anthropic. [Report](#)  
Shared snapshot may contain attachments and data not displayed here.

Provide a percentage of ransomware victims by platform, such as Windows, Macs, and Linux.

Searched the web ›

Here's a breakdown of ransomware victims by platform, based on the most recent available data:

## 📊 Ransomware Attacks by Operating System

### Windows — ~87-92%

Windows was the most affected operating system by ransomware attacks, accounting for **92% of attacks** in 2023 — up from 71% in 2022, according to Trend Micro data via Statista. 85% of managed service providers (MSPs) confirm Windows as the most frequently targeted OS, largely because Windows-based computers are more affordable, more widely used, and often left unpatched.

### Linux — growing, but undercounted

Linux accounts for only **~1.3% of global malware detections** in 2025 — but this figure requires context. Attacks on Linux servers via SSH brute force, webshells, and ransomware have increased significantly, particularly targeting cloud and virtualized infrastructure. Linux ransomware attacks increased **62% between 2022 and 2023**, with ESXi (VMware) servers facing average ransom demands of \$5 million.

### macOS — ~5-7%

macOS accounted for approximately **5% of ransomware attacks** in 2023, according to Statista/Trend Micro. A separate Statista study puts macOS even higher at **7% of attacks**, while also noting that Android (7%) and iOS (4%) are increasingly targeted on mobile.

## ⚠️ Important Context

These numbers can be misleading for a few reasons:

- **Linux is underrepresented in endpoint stats** because most Linux targets are *servers*, not desktops — and many incidents go unreported or aren't captured by consumer antivirus tools.
- Windows may dominate current ransomware infections, but **Linux and macOS variants are actively being developed** by threat actors. Ransomware is increasingly targeting ESXi hypervisors and cloud services.
- Linux powers **49.2% of global cloud workloads** and all of the world's top 500 supercomputers, making it a high-value target even if raw detection numbers are lower.

**Bottom line:** Windows remains the overwhelming primary target by volume, but no platform is safe — and Linux/macOS attacks are growing in sophistication and frequency even if they lag in raw percentage terms.

How can one prevent? A successful ransomware attack on a Mac.

Searched the web ›

Here's a comprehensive guide to preventing a successful ransomware attack on your Mac:

## 🛡️ How to Prevent Ransomware on a Mac

### 1. Keep macOS and Apps Updated

Always keep macOS up to date, as updates often include patches for known security vulnerabilities that ransomware could otherwise exploit. Enable automatic updates in System Settings so you never miss a critical patch.

### 2. Only Download Apps from Trusted Sources

Ransomware attacks on macOS often occur when users inadvertently download and install malicious software, believing it to be legitimate — which is why it's essential to only download apps from the macOS App Store or other trusted sources.

### 3. Use a Reputable Security/Antivirus Tool

Mac users should consider using security software from reputable vendors that offer real-time protection, ransomware detection, and malicious file blocking. Options include Malwarebytes, Intego, and BitDefender for Mac.

### 4. Back Up Your Data — Properly

Store backups locally on external drives for quick recovery, in encrypted cloud storage to safeguard data in transit and at rest, and **offline** to prevent ransomware access — ensuring backups cannot be encrypted during an attack. Time Machine is a good starting point, but offline/disconnected backups are the gold standard.

### 5. Be Extremely Cautious with Emails & Links

Avoid opening any dubious-looking email attachments, pay close attention to the sender's address, and never open attachments that prompt you to run macros to view them — if the attachment is infected, doing so will run a malicious macro that gives malware control of your computer.

### 6. Avoid Public Wi-Fi or Use a VPN

To stay protected, avoid using public Wi-Fi for sensitive transactions, or use a secure VPN service. Unsecured networks are a common vector for attackers to intercept traffic or push malicious payloads.

### 7. Never Plug in Unknown USB Devices

Never connect USB sticks or other storage media to your computer if you do not know where they came from — cybercriminals may have infected the storage medium and placed it in a public place to entice somebody into using it.

### 8. Limit Admin Privileges

Many macOS attacks involve administrative privileges — attackers routinely look for ways to exploit privileged accounts to deploy ransomware. A strong mix of endpoint privilege security and application control can block ransomware actors before they can even get started. Use a standard (non-admin) account for everyday tasks.

### 9. Use Strong, Unique Passwords + MFA

Use a password manager to generate unique passwords for every account, and enable multi-factor authentication (MFA) wherever possible. Credential theft is one of the most common entry points for ransomware operators.

## 🚨 If You Suspect an Infection

Disconnect your Ethernet cable, turn off your Wi-Fi, run a comprehensive antivirus scan, remove any detected threats immediately, and copy unencrypted files to an external drive. You should **never pay the requested ransom** — sending money to criminals offers no guarantee that they will actually unlock your device.

The bottom line: no Mac is immune, but combining good habits (careful downloads, phishing awareness) with technical safeguards (backups, updates, security software, limited admin access) dramatically reduces your risk.

How good is patrick Wardle's RansomWhere at stopoing ransomware?

Searched the web ›

RansomWhere? is a genuinely respected tool from a highly credible source, but it has real strengths and real limitations worth understanding clearly.

## 🔒 Patrick Wardle's RansomWhere? — An Honest Assessment

### Who Made It & What Is It?

RansomWhere? was created by Patrick Wardle, a former NSA staffer and director of research at security firm Synack. It's designed to detect and block the encryption of files by untrusted processes. The tool monitors users' home directories and detects when encrypted files are rapidly being created — a telltale sign of ransomware activity. When such activity is detected, RansomWhere? determines the responsible process and suspends it.

It's now maintained through his non-profit, the **Objective-See Foundation**, and is completely free and open source.

### ✅ What It Does Well

**Behavior-based, not signature-based (in concept)** RansomWhere? continuously analyzes file entropy to identify encryption activity in real time, detecting suspicious processes and stopping ransomware before it can do serious damage. Because it looks for *behavior* rather than known malware signatures, it can in theory catch brand-new ransomware strains.

**Proven against real threats** When LockBit ransomware developed a macOS variant, Wardle noted that RansomWhere? — despite being a bit dated — had no problem generically detecting and stopping LockBit's ransomware even with no prior knowledge of the threat.

**Confirmed lab testing** ZDNet tested the utility and confirmed that it does detect and prevent the KeRanger ransomware from encrypting files.

### ⚠️ Known Limitations

**It's reactive, not proactive** The tool is inherently reactive, so ransomware will likely encrypt a few files — ideally only two or three — before being detected and blocked.

**Limited monitoring scope** RansomWhere? only monitors users' home directories, so malicious activity outside these directories may go unblocked.

**Can be bypassed** If a new piece of macOS ransomware was designed to specifically bypass RansomWhere?, it would likely succeed — particularly if it hijacks or injects code into Apple-signed applications and uses them to encrypt files.

**Signature update gaps** RansomWhere? relies on heuristic and signature-based detection which can be bypassed by modern ransomware techniques, and it lacks frequent automatic updates for detection signatures.

**Trust model has a blind spot** RansomWhere? explicitly trusts binaries signed by Apple. This is a double-edged feature — it helps reduce false positives, but if ransomware is already present on the system before RansomWhere? is installed, it may not be detected.

## 📌 Bottom Line

RansomWhere? is a **solid, free, first line of defense** from one of the world's most respected Mac security researchers. It's particularly good at catching generic or novel ransomware behaviorally. However, it's best thought of as **one layer in a broader security strategy** — not a complete solution on its own. Pair it with regular offline backups, macOS updates, and cautious browsing habits for the most robust protection.

🗒️

Ask Claude your own question